



A Dynamic Hybrid Stacking Approach for Real-Time Threat Detection in High-Mobility Vehicular Networks

A. Hemantha Kumar^{1*}, Bodanapu Jafeer², Madathala Guru Eswar Reddy², Mamuduru Sumanth²

¹Assistant Professor, ²UG Student, ^{1,2}Department of Electronics and Communication Engineering

^{1,2}Geethanjali Institute of Science and Technology, Nellore-Bombay Highway, S.P.S.R, Andhra Pradesh 524137, India

*Correspondence: A. Hemantha Kumar

Abstract

Vehicular Ad Hoc Networks (VANETs) have become a fundamental part of modern intelligent transportation systems, enabling vehicles to communicate for improved safety and traffic management. Historically, early network security mechanisms in vehicular systems relied on manual monitoring and rule-based approaches to identify malicious activities. However, with the rapid expansion of connected vehicles, these traditional manual systems are no longer sufficient to handle complex and large-scale network data. The major problem lies in accurately detecting malicious nodes involved in attacks such as Denial of Service (DoS), Sybil, and Blackhole, which can severely disrupt communication and compromise system reliability. Manual detection methods are time-consuming, error-prone, and lack scalability, making them ineffective in dynamic and high-mobility VANET environments. This creates a strong need for automated, intelligent, and adaptive detection systems. To address this challenge, the proposed system introduces a Flask-based malicious node detection framework that leverages machine learning models including AdaBoost (AB), Logit Boosting (LB), Gradient Boosting (GB), and Natural Gradient Boosting (NGB). The system incorporates automated preprocessing, real-time exploratory data analysis, and multi-target classification to improve detection accuracy. Among these, NGB demonstrates superior performance, achieving accuracies of 97.61% for DoS attacks, 97.96% for Sybil attacks, and 96.70% for Blackhole attacks due to its probabilistic learning capability and ability to handle uncertainty. The proposed system significantly enhances detection efficiency and accuracy, providing a scalable and user-friendly solution that strengthens network security and ensures reliable communication in intelligent vehicular environments.

Keywords: Network security, Malicious node detection, VANETs, Machine learning, Natural gradient boosting classification.

1. Introduction

The steady growth of the global automotive cybersecurity market from 2022 to 2032, showing a clear upward trend in total market size. Starting at around USD 3.2 billion in 2022, the market expands consistently each year and is projected to reach approximately USD 22.2 billion by 2032. This growth reflects the increasing reliance of modern vehicles on digital communication, software-driven functions, and external connectivity, all of which require stronger protection measures. The overall rise also indicates that cybersecurity has become an essential

component of automotive system design rather than a secondary consideration. Figure 1 also highlights the role of cloud-based analytics, where vehicle data is sent for centralized monitoring, processing, and system-level coordination. This cloud layer supports large-scale data handling and provides insights that can enhance vehicle performance and overall traffic management. At the same time, the image illustrates a potential threat scenario in which an intruder attempts to inject fake or manipulated data into the communication channel alongside genuine information. Such interference can distort the vehicle's perception



of its surroundings, leading to incorrect interpretations of traffic conditions or object positions. This visual representation emphasizes the importance of maintaining data integrity and reliability in autonomous electric vehicle systems. It shows that while extensive connectivity and data sharing significantly improve vehicle awareness and operational efficiency, they also introduce vulnerabilities that must be addressed to ensure safe, stable, and trustworthy vehicle operation within connected road networks.

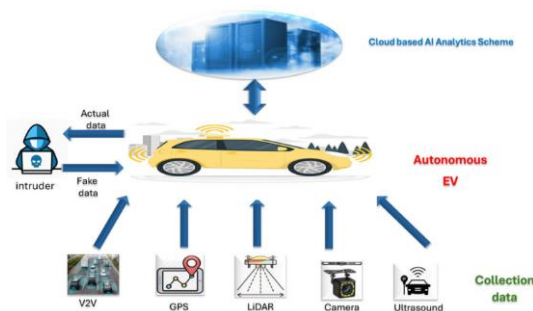


Figure. 1: An intelligent attack detection framework for the internet of autonomous vehicles.

The stacked structure of the bars highlights the contribution of different security areas such as wireless, network, endpoint, application, and cloud security. Network and wireless security form a major share throughout the timeline, emphasizing the importance of safeguarding vehicle communication channels. Over time, application and cloud security segments grow more noticeably, aligning with the increasing use of cloud-based services and in-vehicle software platforms. Together, these trends show a shift toward comprehensive, multi-layered security coverage as the automotive ecosystem becomes more connected and data driven.

2. LITERATURE SURVEY

Kanwal Rashid et al. [1] addressed the ongoing development of modern vehicular communication and the critical security challenges present in VANET. It focused on detecting malicious nodes, particularly those involved in DoS attacks that disrupt

communication by overwhelming targeted vehicles. A real-time malicious node detection system was proposed using a distributed multi-layer machine learning classifier. The system was evaluated through OMNET++ and SUMO simulations using GBT, LR, MLPC, RF, and SVM models on datasets comprising normal and attacking vehicles. The results demonstrated high classification performance, achieving 99% accuracy overall, with LR and SVM reaching 94% and 97%, respectively, and RF and GBT attaining 98% and 97%. The integration of Amazon Web Services further enhanced network performance by preventing increases in training and testing time as network nodes scaled.

Varun P. Sarvade et al. [2] proposed architecture incorporated hybrid Classical–Quantum Machine Learning (QML) methods for detecting DoS threats. Three QML methods C-QNN, C-QBM, and C-QKM were examined. Emulations were conducted on a custom-built vehicular network with random movements and speeds between 0 and 100 km/h, and performance was evaluated on two datasets. The results showed that the hybrid C-QNN model performed better than the other two approaches. It achieved 99% accuracy on the UNB-CIC-DoS dataset and 90% accuracy on the Kaggle DoS dataset. Jing Chen et al. [3] proposed a blockchain based malicious node detection mechanism that relied on consensus, identity verification, message integrity checking, and false message identification. Using public–private keys, RSA encryption, and a blockchain-driven identification algorithm, the system verified vehicle identities and message authenticity. Simulation results showed that the proposed mechanism significantly improved malicious node detection accuracy, false message identification, and overall network performance.

Ahmad Aloqaily et al. [4] achieved an accuracy of 99.995% with a false positive rate of 0.00001%, significantly outperforming



traditional methods. Furthermore, the approach was highly robust against newly emerging attack patterns and adaptable to varying computational constraints. Overall, the research represented a major advancement toward scalable, real-time cybersecurity solutions for next-generation vehicles. Safi Ullah et al. [5] proposed a hybrid deep learning model based on LSTM and GRU for cyberattack detection. The model was evaluated using a combined DoS dataset and a car-hacking dataset. The experimental results showed that the model achieved detection accuracies of 99.5% for DoS attacks and 99.9% for car-hacking attacks. These results, along with high precision, recall, and F1-scores, demonstrated the superior performance of the proposed framework.

Mohamed Sayed Farghaly et al. [6] followed a three-phase methodology that included reviewing 16 peer-reviewed sources, applying CVSS 4.0 scoring to 15 attack types, and evaluating four generative AI models using 117 annotated vulnerabilities. Expert validation showed that LiDAR sensors were the most vulnerable, followed by radar and ultrasonic sensors. Network-based attacks dominated the dataset, with most requiring low complexity and no user interaction. The most severe attack vectors identified were eavesdropping, Sybil attacks, and replay attacks. Performance results indicated that DeepSeek achieved the highest accuracy on network-based attacks, while all AI models struggled with minority classes, underscoring the need for improved vulnerability assessment approaches. Mostafa Mahmoud El-Gayar et al. [7] proposed specifically for IoV security. The model employed data-balancing techniques and dimensionality reduction to enhance detection capability. Experimental evaluations demonstrated strong performance across multiple datasets. The DFSENet achieved high accuracy and reliability, establishing it as an effective solution for protecting IoV systems against cyber-attacks.

Junhai Cao et al. [8] study investigated connectivity reliability in VANETs by analysing node movement characteristics and failure modes. Nodes within VANET clusters exhibited interactive relationships and followed regular movement patterns rather than random mobility models. The identified failure modes included hardware and software failures, energy depletion, intentional attacks, and isolation failures. A routing path identification algorithm was proposed to optimize node communication energy consumption. MATLAB simulations confirmed the effectiveness of the approach and showed that attraction distance influenced isolation failure and connectivity reliability. Muawia A. Elsadig et al. [9] proposed Random Forest based model demonstrated superior performance in accuracy, computational cost, and error rate compared to benchmark classifiers. It achieved 99.8% accuracy with minimal processing time and negligible classification errors, outperforming all existing techniques.

Yonas Teweldemedhin Gebrezgiher et al. [10] reviewed existing research applying machine learning, blockchain, and cryptographic techniques to secure V2X communications, highlighting key security challenges and identifying gaps in current ML, Blockchain, and MEC-based solutions. Finally, it outlined a conceptual framework integrating machine learning, blockchain, and MEC, and identified future research directions to address evolving V2X security threats. Sakibul Islam et al. [11] revealed a dominant reliance on centralized, supervised learning approaches and standard datasets, which limited their applicability to real-world UAV operations. Deep learning techniques demonstrated strong detection accuracy but often operated under ideal conditions and lacked resilience to zero-day attacks and real-time constraints. Emerging trends indicated a shift toward lightweight IDS models and federated learning frameworks for scalable and privacy-preserving UAV security. The review identified critical research gaps,



including the lack of real UAV datasets, absence of standardized benchmarks, and limited exploration of lightweight detection approaches. These findings provided a foundation for advancing secure and resilient UAV systems.

Brooke Lampe et al. [12] study emphasized that intrusion detection became critical when such vulnerabilities were exploited. It reviewed a wide range of threats and intrusion detection techniques from in-vehicle networks to the broader IoV. The paper concluded that intrusion detection systems offered a cost-effective and non-intrusive solution for enhancing automotive security and safety. Hetong Wang et al. [13] study also showed how adversaries could exploit open wireless channels and AI-driven RIS control through adversarial perturbations, leading to misclassification and system disruption. Despite these vulnerabilities, RIS was shown to enhance security and privacy in RF and VLC systems. The survey emphasized the need for robust, cost-effective security frameworks and cross-layer defence strategies to ensure secure RIS deployment.

Wadii Boulila et al. [14] proposed a misbehaviour-aware on-demand collaborative intrusion detection system (MACIDS). The proposed approach was based on distributed ensemble learning, where vehicles independently trained local intrusion detection models using the random forest algorithm. The method aimed to improve intrusion detection accuracy while mitigating the impact of malicious collaborators. Breno Sousa et al. [15] study simulated realistic 5G vehicular networks using NS3 and mobility patterns generated with SUMO. Multiple datasets were created by varying the number of vehicles, attackers, and mobility conditions. The results showed that the proposed IDS achieved high performance, with F1 scores of 1.00 using decision trees and 0.98 using random forests.

3. Proposed System

The proposed system architecture, as shown in the flowchart, provides an end-to-end framework for securing vehicular networks against cyber-attacks by combining data-driven analysis and advanced learning models. It begins with the collection of vehicular network data encompassing mobility, communication, trust, and attack-related features generated through V2V, V2I, and V2X interactions. This data undergoes preprocessing to remove noise, normalize feature scales, and encode heterogeneous attributes into a structured format suitable for analysis. Exploratory data analysis is then performed to understand traffic behaviour, identify attack patterns, and analyse feature correlations that distinguish normal and malicious activities. The processed data is subsequently fed into both baseline boosting models for comparative evaluation and the proposed NGB classifier, which uses natural gradient optimization to produce probabilistic predictions while explicitly modelling uncertainty, as shown in figure 2. Based on these predictions, a multi-attack detection module identifies Sybil, DoS, and Black Hole attacks in real time. Finally, the system generates timely alerts with reduced false alarms, enabling effective mitigation actions and resulting in a secure and reliable vehicular network.

Vehicular Network Data Collection: The architecture begins with the collection of heterogeneous vehicular network data generated from V2V, V2I, and V2X communications. This data includes mobility features (speed, position, acceleration), communication features (packet rate, delay, bandwidth usage), trust-related features (node reputation, message consistency), and attack-related indicators. Because vehicular environments are highly dynamic, the collected data is large-scale, high-speed, and time-sensitive, forming the foundation for intelligent intrusion detection.

Data Preprocessing: Raw vehicular data is often noisy, incomplete, and inconsistent due to



wireless channel variations and high vehicle mobility. The preprocessing module cleans and transforms this data to make it suitable for learning models. Noise reduction removes outliers and corrupted packets, normalization scales features to a common range to avoid bias toward dominant attributes, and feature encoding converts categorical or protocol-specific fields into numerical representations. This step ensures data reliability and improves learning efficiency.

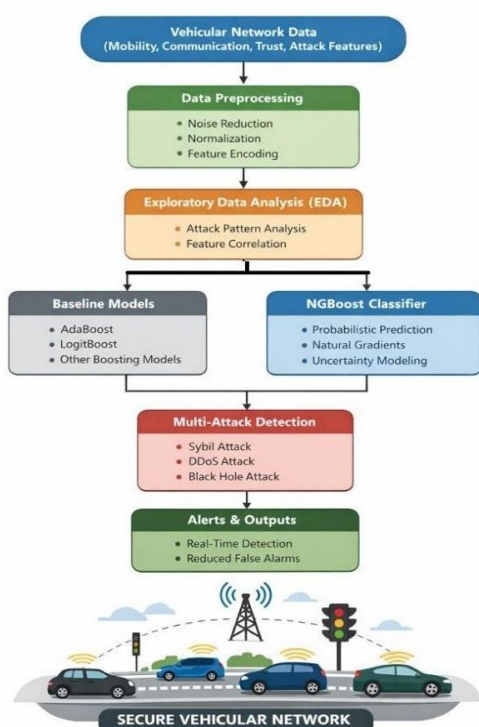


Figure 2: Proposed system architecture.

Exploratory Data Analysis (EDA): EDA is performed to understand the underlying patterns and relationships within the vehicular dataset. Attack pattern analysis helps identify Behavioural differences between normal and malicious traffic, such as abnormal message frequency or route manipulation. Feature correlation analysis examines dependencies among features, enabling the selection of informative attributes and reducing redundancy. This stage provides insights that guide effective model training.

Model Layer: The architecture includes two parallel modelling paths for performance comparison.

- **Baseline models:** Traditional boosting-based classifiers such as AB, LB, and GB are used as reference methods. These models focus on improving classification accuracy by iteratively correcting misclassified samples but lack explicit uncertainty modelling.
- **NGB classifier (proposed model):** NGB introduces probabilistic prediction by estimating full conditional probability distributions rather than point predictions. Using natural gradients, it ensures stable and efficient optimization. Uncertainty modelling is a key advantage, allowing the system to quantify confidence in predictions, which is crucial in safety-critical vehicular networks.

Multi-Attack Detection Module: Outputs from the trained models are used to detect multiple attack types simultaneously. The system is designed to identify Sybil attacks (fake identity generation), DoS attacks (flooding to disrupt communication), and Black Hole attacks (malicious packet dropping or route manipulation). This multi-attack capability makes the architecture robust against diverse and coordinated threats in vehicular environments.

Alerts and Outputs: Once an attack is detected, the system generates real-time alerts to vehicles and roadside infrastructure. The probabilistic nature of NGB helps reduce false alarms by considering prediction confidence. This module ensures timely response, enabling vehicles and network controllers to take preventive or corrective actions.

Secure Vehicular Network Outcome: The outcome of the architecture is a secure and reliable vehicular network. By combining intelligent preprocessing, detailed data analysis, advanced probabilistic learning, and multi-attack detection, the system enhances



road safety, communication reliability, and trustworthiness of vehicular networks under both normal and adversarial conditions.

4. Results Analysis

A result analysis is a critical stage in any study or experiment, where collected data is carefully examined and interpreted to draw meaningful conclusions. It involves organizing the results, identifying patterns, trends, and relationships, and comparing them with the expected outcomes or hypotheses. Through systematic evaluation, result analysis helps in understanding whether the objectives of the study have been achieved. It also highlights any discrepancies, errors, or unexpected findings that may require further investigation. By providing logical explanations and insights, this process strengthens the validity and reliability of the research. Ultimately, result analysis serves as the foundation for making informed decisions and recommendations based on the findings.

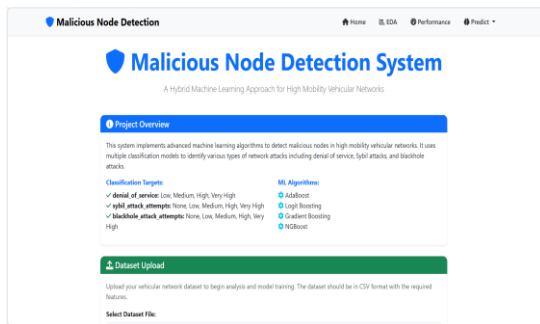


Figure. 3: Malicious node detection system interface overview.

Figure 3 illustrates the interface of a malicious node detection system designed for high mobility vehicular networks, highlighting its integrated machine learning framework for identifying network threats. The figure depicts a structured dashboard that provides an overview of the system's functionality, including classification targets such as DoS, Sybil, and blackhole attacks with varying intensity levels. It showcases the utilization of multiple machine learning algorithms, including ensemble and boosting techniques, to enhance detection accuracy and robustness.

The representation emphasizes the system's capability to process vehicular network data and support predictive analysis through a centralized platform. Furthermore, the figure conveys the workflow beginning with dataset upload, enabling data-driven analysis and model training for effective malicious node detection. Figure 4 illustrates the DoS classification results generated by different machine learning models, presenting a comparative analysis of their performance across multiple evaluation metrics. The figure depicts the effectiveness of algorithms such as AB, LB, GB, and NGB in classifying attack intensity levels, highlighting variations in accuracy and prediction consistency. It showcases confusion matrices for each model, enabling a detailed assessment of classification outcomes across categories such as normal, medium, high, and very high. The representation emphasizes the superior performance of NGB, demonstrating high precision and balanced predictions compared to other models. Furthermore, the figure conveys the overall evaluation framework used to measure model reliability and effectiveness in detecting DoS attacks within vehicular networks.

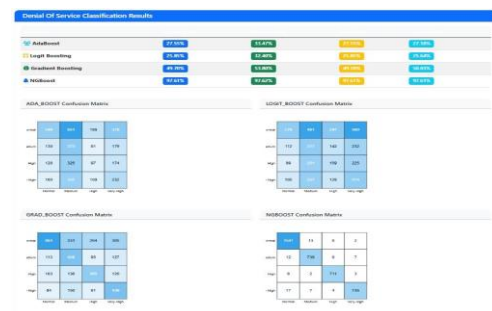


Figure. 4: Confusion matrix obtained for DoS attack classification results.

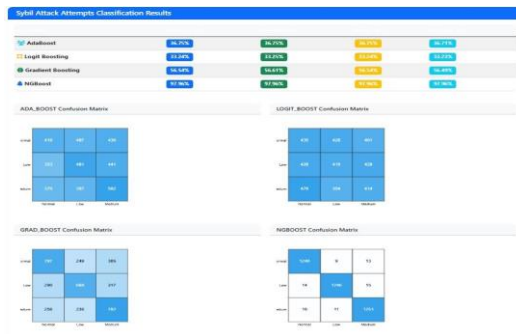


Figure. 5: Confusion matrix obtained for Sybil attack attempts classification results.

Figure 5 illustrates the classification results of Sybil attack attempts using multiple machine learning models, providing a comprehensive comparison of their predictive performance. The figure depicts the evaluation of algorithms such as AB, LB, GB, and NGB across key metrics including accuracy, precision, recall, and F1-score. It showcases confusion matrices for each model, enabling detailed insight into how effectively each algorithm classifies different levels of Sybil attack attempts, such as normal, low, and medium. The representation highlights the improved consistency and higher prediction capability of NGB compared to other models. Furthermore, the figure conveys the effectiveness of the proposed approach in accurately identifying Sybil attack patterns within vehicular network environments. Figure 6 illustrates the classification results of blackhole attack attempts using various

machine learning algorithms, highlighting their comparative effectiveness in detecting different attack intensity levels. The figure depicts the performance of models such as AB, LB, GB, and NGB across evaluation metrics including accuracy, precision, recall, and F1-score. It showcases confusion matrices for each algorithm, providing a detailed understanding of how well each model classifies categories such as normal, low, medium, high, and very high attack levels. The representation emphasizes the superior predictive capability and consistency of NGB, demonstrating its effectiveness in minimizing misclassification. Furthermore, the figure conveys the robustness of the proposed system in accurately identifying blackhole attack patterns within vehicular network environments.

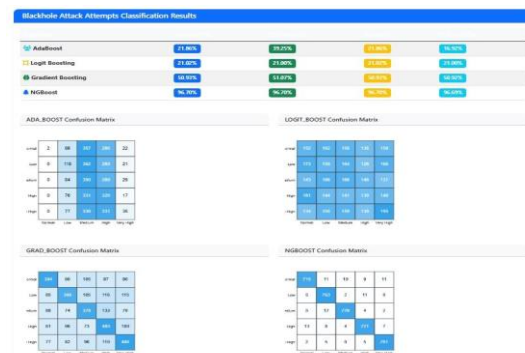


Figure. 6: Confusion matrix obtained for blackhole attack attempts classification results

Table: 1. overall performance metrics for each algorithm across the three different attack types.

Attack Type	Algorithm	Accuracy	Precision	Recall	F1-Score
DoS	AB	27.55%	33.47%	27.55%	27.18%
	LB	25.85%	32.40%	25.85%	25.64%
	GB	49.70%	53.80%	49.70%	50.03%
	NGB	97.61%	97.62%	97.61%	97.61%
Sybil Attack	AB	36.75%	36.75%	36.75%	36.71%
	LB	33.24%	33.25%	33.24%	33.23%
	GB	56.54%	56.61%	56.54%	56.49%
	NGB	97.96%	97.96%	97.96%	97.96%



Blackhole Attack	AB	21.86%	39.25%	21.86%	16.92%
	LB	21.02%	21.00%	21.02%	21.00%
	GB	50.93%	51.07%	50.93%	50.92%
	NGB	96.70%	96.70%	96.70%	96.69%

Table 1 presents a performance comparison of multiple machine learning algorithms across three attack types, with accuracy serving as a key evaluation metric. For DoS attacks, AB achieves an accuracy of 27.55%, while Logit Boosting (LB) records a slightly lower accuracy of 25.85%, indicating limited effectiveness of these models for this attack category; GB shows moderate improvement with an accuracy of 49.70%, whereas NGB significantly outperforms all others with a remarkably high accuracy of 97.61%, demonstrating superior detection capability. In the case of Sybil attacks, AB achieves an accuracy of 36.75% and LB records 33.24%, both reflecting relatively low classification performance; GB improves the accuracy to 56.54%, while NGB again delivers outstanding results with an accuracy of 97.96%, highlighting its consistency across attack types. For Blackhole attacks, AB and LB show poor performance with accuracies of 21.86% and 21.02% respectively, while GB achieves a moderate accuracy of 50.93%; however, NGB once more dominates with an accuracy of 96.70%, confirming its robustness and reliability in accurately detecting various types of network attacks.

5. Conclusion

The developed Flask-based VANET malicious node detection system demonstrates that NGB is the most effective and dependable algorithm for enhancing security in vehicular network environments. Experimental results consistently show that NGB achieves superior accuracy across all attack types, with 97.61% for DoS, 97.96% for Sybil attacks, and 96.70% for Blackhole attacks. Its strong performance is

primarily due to its probabilistic learning approach using natural gradients, which enables it to efficiently manage highly correlated features such as `trust_score` and `neighbor_trust_score_avg`. In contrast, traditional models like GB deliver only moderate performance with an average accuracy of approximately 52.39%, while AB and LB perform poorly, remaining below 37% accuracy. Additionally, NGB exhibits highly reliable classification behavior, as evidenced by its confusion matrices, where it maintains high correct predictions with minimal misclassification. The study also highlights the importance of a well-structured and modular pipeline that incorporates automated preprocessing, real-time exploratory data analysis, and multi-target learning to address the dynamic and complex nature of VANET systems. A clear performance advantage is observed, with NGB outperforming GB by nearly 45% in accuracy, demonstrating the effectiveness of probabilistic boosting over conventional techniques. This advantage becomes particularly critical in high-mobility scenarios where parameters such as `packet_drop_ratio`, latency, and `signal_strength` change rapidly. The proposed system provides a highly accurate, scalable, and user-friendly framework for detecting and classifying malicious node activities, ensuring improved network security and reliable operation in intelligent vehicular environments.

References

- [1] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An Adaptive Real-Time Malicious Node Detection Framework Using Machine



- Learning in Vehicular Ad-Hoc Networks (VANETs),” *Sensors*, vol. 23, no. 2594, 2025.
- [2] V. P. Sarvade, S. A. Kulkarni, and C. V. Raj, “A Hybrid Classical-Quantum Neural Network Model for DoS Attack Detection in Software-Defined Vehicular Networks,” *Information*, vol. 16, no. 722, 2025.
- [3] J. Chen, T. Li, and R. Zhu, “Analysis of Malicious Node Identification Algorithm of Internet of Vehicles under Blockchain Technology,” *Applied Sciences*, 2025.
- [4] A. Aloqaily, E. E. Abdallah, A. Baarah, M. Alnabhan, E. Alshdaifat, and H. Milhem, “Optimized Hybrid Ensemble Intrusion Detection for VANET-Based Autonomous Vehicle Security,” *Network*, vol. 5, no. 43, 2025.
- [5] S. Ullah, M. A. Khan, J. Ahmad, S. S. Jamal, Z. e Huma, M. T. Hassan, N. Pitropakis, A. Arshad, and W. J. Buchanan, “HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles,” *Sensors*, vol. 22, no. 1340, 2022.
- [6] M. S. Farghaly, H. K. Aslan, and I. T. Abdel Halim, “A Hybrid Human-AI Model for Enhanced Automated Vulnerability Scoring in Modern Vehicle Sensor Systems,” *Future Internet*, vol. 17, no. 339, 2025.
- [7] M. M. El-Gayar, F. A. F. Alrslani, and S. El-Sappagh, “Smart Collaborative Intrusion Detection System for Securing Vehicular Networks Using Ensemble Machine Learning Model,” *Information*, vol. 15, no. 583, 2024.
- [8] J. Cao, Y. Bian, C. He, F. Liu, D. Xu, and Y. Guo, “Evaluation of Connectivity Reliability of VANETs Considering Node Mobility and Multiple Failure Modes,” *Sensors*, vol. 25, 2025.
- [9] M. A. Elsadig, A. Altigani, Y. Mohamed, A. H. Mohamed, A. Kannan, M. Bashir, and M. A. E. Adiel, “Connected Vehicles Security: A Lightweight Machine Learning Model to Detect VANET Attacks,” *World Electric Vehicle Journal*, vol. 16, no. 324, 2025.
- [10] Y. T. Gebrezgiher, S. R. Jeremiah, X. Deng, and J. H. Park, “Machine Learning-Based Blockchain Technology for Secure V2X Communication: Open Challenges and Solutions,” *Sensors*, 2025.
- [11] M. S. Islam, A. S. Mahmoud, and T. R. Sheltami, “AI-Enhanced Intrusion Detection for UAV Systems: A Taxonomy and Comparative Review,” *Drones*, vol. 9, no. 682, 2025.
- [12] B. Lampe and W. Meng, “Intrusion Detection in the Automotive Domain: A Comprehensive Review,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2356–2426, 2023.
- [13] H. Wang et al., “Navigating the Dual-Use Nature and Security Implications of Reconfigurable Intelligent Surfaces in Next-Generation Wireless Systems,” *IEEE Communications Surveys & Tutorials*.
- [14] W. Boulila, “Misbehavior-Aware On-Demand Collaborative Intrusion Detection System Using Distributed Ensemble Learning for VANET,” *Electronics*, 2020.
- [15] B. Sousa, N. Magaia, and S. Silva, “An Intelligent Intrusion Detection System for 5G-Enabled Internet Vehicles,” *Electronics*, vol. 12, no. 1757, 2024.